DOI: 10.38146/BSZ.2019.1.9

HAZAI LÁSZLÓNÉ DR.

Módszerek, technikák a biometrikus arcfelismerésben, -azonosításban

Az emberek egyedi, tudományosan igazolt, fiziológiai vagy viselkedésalapú jellegzetességeit felhasználó, mérhető, az egyéni azonosítást lehetővé tevő módszert nevezzük biometriának. A biometrikus azonosítás az e megkülönböztethető jellegzetességeken alapuló, napjainkban igen széles körben és területen használt – általában a biztonság megerősítését támogató – módszereket magában foglaló gyűjtőfogalom.

Az ember mérhető adottságai, jellegzetességei például az ujjlenyomat, a tenyérlenyomat, az írisz mintázata, az erek mintázata a retinában, az ujjban, a tenyérben, a hangképzés jellemzői, illetve a testrészek (arc, fül, kéz) geometriája, biológiai, fizikai jellemzői, valamint egyes viselkedésalapú jellemzők, mint például a járás, testtartás stb. Az egyes jellegzetességek, sajátosságok matematikai módszerekkel, algoritmusokkal írhatók le. Az így kapott biometrikus adat *(template)* egy olyan gépi kód, amely lehetővé teszi az összehasonlítást[1].

Egy biometrikus azonosítási módszer hatékonysága egyrészt attól függ, hogy mely biometrikus sajátságokat kívánjuk mérni, a mérést milyen pontossággal tudjuk elvégezni, illetve nagyon nagy mértékben természetesen attól, hogy az adott sajátság mennyire egyedi, mennyire jellemző egy adott személyre, és fontos az is, hogy mennyire állandó. Másrészt meghatározza a módszer eredményességét, hogy milyen algoritmusokat használ a biometrikus minták generálására és milyet az összehasonlításra.

A biometrikus elemek személyazonosításra történő tömeges, illetve automatikus alkalmazása és ezzel összefüggésben a kapott eredmények értékelése sok paraméter, körülmény vizsgálatát, figyelembevételét igényli. A technikai részletek kidolgozását mindig meg kell hogy előzze annak eldöntése, milyen célból, miért van szükség a biometrikus azonosításra, ez után vizsgálni kell a *biztonság kérdését, amely magában foglalja* a szükségesség és az arányosság szempontjait, a biometrikus azonosító hamisíthatóságának kérdését, a mérések pontosságát és megbízhatóságát, az ebből eredő hibák nagysá-

1 ICAO Doc 9303 Machine Readable Travel Documents. 2015, part 9.

gát. Fontos továbbá vizsgálni az *alkalmasság, alkalmazhatóság* aspektusait, amely olyan, a gyakorlatban fontos kérdések elemzését takarja, mint a biometrikus azonosítók mérésének gyorsasága, hitelessége, megismételhetősége, a mérés bonyolultsága, a mérő eszközök bonyolultsága, mérete, költsége, a mérést befolyásoló egyéb tényezők, a kockázatok ismerete, a módszer elfogadottsága stb.

Ezzel párhuzamos, szintén nem kevésbé összetett feladat a *kivitelezés, a további technikai kérdések* (például milyen adat és milyen formátumban tárolódjon, az adat tárolására alkalmas adathordozó típusának kiválasztása), valamint a *biztonsági követelmények* kidolgozása (például a tárolt adatokhoz való hozzáférés, a hitelesítés rendje).

A biometrikus azonosítás irányait, módszereit, ezek fejlődését vizsgálva megállapítható, hogy az elmúlt évtizedben visszatérően igen nagy figyelmet, érdeklődést kapott az arcfelismerés és -azonosítás. Nagyon sok kutató foglalkozik a témával már hosszú ideje, és a mesterséges intelligencia, az okosalkalmazások lehetősége napjainkban újabb lendületet adott a kutatásoknak.

Az ok nyilvánvaló, hiszen ez az úgynevezett passzív azonosítást lehetővé tevő, sokféle területen és célra használható eljárás a leginkább elfogadott biometrikus módszer, mert nem igényli a személy aktív közreműködését, emellett gyors, és tömegeseményeknél távoli azonosításra is alkalmazható. Tény azonban, hogy az elmúlt néhány évtizedben olykor pozitív, máskor negatív vélemények születtek a rendszerek alkalmasságának, használhatóságának a megítélését illetően.

A biometrikus azonosítást végző rendszerek hatékonysága nagymértékben a választott biometrikus jellemző emberenkénti egyediségétől és az adott jellemző mérésének pontosságától függ.

Nem szerencsés olyan biometrikus sajátosságokat választani, amelyek nehezen vagy csak nagy hibával mérhetők.

A biometrikus azonosítók közül az arcazonosítás a kényelmi szempontokat figyelembe véve optimális, de megbízhatósága kimutathatóan elmarad a többi biometrikus azonosító jelentős részétől. Ahhoz, hogy mely tényezők játszanak ebben jelentős szerepet, ismerni szükséges a technológiát, hogy az egyes technológiai lépések, a választott paraméterek, a különböző döntési folyamatok ismeretében megfelelően értékelni tudjuk a kapott eredményeket.

Ha az arcazonosítást összevetjük más biometrikus azonosítással, megállapítható, hogy az arcalapú azonosítás esetében a variabilitás, a pozíciók, a beállítások, a megvilágítás minősége, a gyűjtött, illetve a mintaképek felbontá-

sára, minőségére (zajosságára) való érzékenység nagymértékben befolyásolja a rendszerek eredményességét.

Hibát okozhat számtalan, ma még meg nem magyarázott tényező, például egyes rendszerek jobb eredményt mutathatnak a nők azonosítása esetében, mint a férfiaknál, vagy hasonló probléma állhat elő idősebb, illetve fiatal emberek vonatkozásában, vagy különböző bőrszín esetében. Téves elfogadás történhet, ha az adatbázisban tárolt fotóhoz képest változott a személy hajviselete, a hajszíne. Az ergonómiai tényezők mellett hatással lehet az eredményre az a környezet, amelyben használjuk az adott rendszert, és azoknak az eszközöknek az állapota, amelyeket a rendszer használ. Hibát okozhat, ha alacsony felbontású kamerával készült az összehasonlítás alapjául szolgáló fotó.

Laboratóriumi körülmények között, szigorúan ellenőrzött és kézben tartott paraméterek mellett, elfogadott technológiát, algoritmusokat alkalmazva az arc detektálásának hibája öt és tíz százalék között változik[2]. Érdemes tehát a célokat ennek tudatában meghatározni, dönteni az alkalmazás körülményeiről, értelmezni az azonosság kérdésének – elfogadás vagy elutasítás – biztonságra gyakorolt hatását.

Az arcazonosítás folyamata képfeldolgozás, képanalízis, amelynek első fontos lépése az *arc felismerése a képen (detektálás),* ez az optikai adatfelvételezés – a mozgó (videófolyam) vagy az álló képek rögzítése kamerák segítségével – után különböző, általános (szűrés, szegmentálás stb.) és az arcazonosítást támogató speciális képfeldolgozási módszerekkel (algoritmusokkal) történik. Az arc felismerését támogató, ismert speciális képfeldolgozási eljárások, detektáló módszerek például[3]:

– a bőrszín alapján történő keresés (például RGB[4] alapszínek alapján, a bőrszín homogén színkülönbségi értékeinek segítségével);
– template-illesztés módszerével, ami lehet például egy mintázatalapú felismerés (például világos és sötét régiók, foltok keresése egy adott felületen, ezt nevezik fényességalapú felismerésnek *[brightness based recognition],* vagy kontúr, sziluett alapján, amelyet jellemzőalapú felismerésnek *[feature based recognition]* neveznek); vagy

2 https://www.gemalto.com/govt/inspired/biometrics

3 Távoli személyazonosítási technikák. Budapesti Műszaki és Gazdaságtudományi Egyetem Méréstechnikai és Információs Rendszerek Tanszék–Gardware Systems Kft., 2005. http://oldweb.mit.bme.hu/eng/research/search/downloads/tst/Irodalomkutatas.pdf

4 RGB-színtér (R: vörös, G: zöld, B: kék), az RGB színtér három alapszín keveréséből létrehozott színkocka. Ebben a háromdimenziós színtérben egy szín háromkomponensű *(r, g, b)* vektorként határozható meg, így létrehozva a kétdimenziós színteret, amely már használható az összehasonlításra.

– statisztikai analízis, gépi tanulás módszere segítségével (például neurális háló alkalmazása, amelyhez először manuálisan rögzítik az arckép egyes elemeit, amelyek a neurális háló számításának kiindulási pontjai).

A detektálás során számos nehézséget kell kezelniük a rendszereknek, mint például

– az arc pozíciójának, beállításának variációit – az ideális pozíció természetesen a szembe pozíció, azonban nyilvánvaló, hogy ritkán megvalósítható ez az ideális kép, ezért ennek a problémának a kezelésében ma már nagyszámú felvételezési módszer és algoritmus nyújt segítséget;
– a mérni kívánt sajátosság takarását, rejtését;
– az arckifejezés változásait;
– a különböző kamerák és a környezet kondícióinak hatását a képi paraméterekre.

Az arcnak a képen való megtalálása után – vagy ezzel párhuzamosan – a rendszer soron következő feladata a biometrikus azonosításhoz szükséges *mérendő és összehasonlítható tulajdonságok kivonása,* összegyűjtése. Ezeknek az algoritmusoknak is általában az arc tulajdonságainak detektálásához alkalmas arcazonosító algoritmusok az alapjai.

Az azonosításhoz szükséges műveletek sora általánosságban a következő módon írható le. A választott biometrikus azonosító, ebben az esetben az arckép *optikai adat felvételezését követő digitalizálás* után jön létre az a képpontokból (pixelekből) álló sokdimenziós tér (*N* dimenziós vektortér), amely a képfeldolgozási műveletek alapjául szolgál, és amelyben *meghatározzuk a minta sajátosságparamétereit, vagyis a koordinátáit, az úgynevezett sajátságvektorokat.* A biometrikus rendszerekben ezeknek a sajátságvektoroknak a segítségével történik meg az *összehasonlítás,* a *hasonlósági (távolsági) mutatók kiszámítása,* majd ez után áll elő a *döntés, az azonosság mértékének a megállapítása.* A döntés a sajátságvektorok távolságértékeiből számolt bináris függvény, ami válasz a két minta hasonlóságának kérdésére. Az eredményt pontosítja, ha az egyes sajátosságokhoz tartozó bizonytalansági faktorokat is ismerjük, és az eredményt ezzel korrigáljuk.

Az úgynevezett multimodális rendszereknél – amikor egy ember különböző biometrikus jellegzetességeinek a mérésére is sor kerülhet – a biometrikus-sajátosság-paraméterek együttes használata is ismert, ebben az esetben a paramétereket egyetlen sajátságvektorba integrálják. Azonban a biometrikus azonosítást végző multimodális rendszerek esetén a gyakorlati megvalósítás

nehézségei miatt ekkor is inkább az egyes egyedi sajátosságok összehasonlítására kerül sor[5].

Osztályozásukat tekintve az arcazonosító algoritmusok lehetnek minta- vagy geometriaalapú algoritmusok.

A mintaalapú arcazonosítási módszerek esetében a teljes kép vagy annak egyes kiemelt részleteinek (például szem, orr, száj) összevetése történik a tárolt mintakép(ek) elemeivel különböző algoritmusok segítségével. Ebben az esetben is sajátságvektorok kivonatolására van szükség, de ezeket nem geometriai módszerek, hanem különböző statisztikai eljárások állítják elő (*eigenface,* legközelebbi szomszéd osztályozás stb.).

Ezek a rendszerek érzékenyek a megvilágításra, erőforrás-igényesek. Hibát okozhat a pixelek intenzitásának eltérése az adatbázis képeihez viszonyítva.

A geometriai módszerrel az egyes képi elemek, arcrészletek (például szem, orr, száj) egymáshoz viszonyított pozíciójának, méretének, alakjának vizsgálatával, összevetésével végzik az azonosítást. A hiba csökkentése érdekében fontos tényező a mért sajátosságok számának helyes megválasztása.

Ezek a rendszerek érzékenyebbek lehetnek a pozícióra, beállításokra, mert nem eléggé pontosak a jellemző azonosítási pontok felvételét illetően.

A különböző módszerek különböző érzékenységgel kezelik az egyes körülményeket, beállításokat.

Gyakran egy arcot detektáló, azonosító módszer nem elégséges a megfelelő eredmény eléréséhez, ezért szükség lehet a különböző módszerek kombinálására is. Ezzel a megoldással napjainkban a fejlesztők élnek is, sok kutatás igazolja, hogy hibrid módszerekkel – többféle algoritmus használatával – jobb eredmény érhető el.

Ahhoz, hogy jó döntés szülessen egy biometrikus azonosító, jelen esetben arcfelismerő azonosító rendszer létrehozásánál – mint említettem –, lényeges szempont, hogy konkrétan meghatározzuk a felhasználás célját. Ha *ellenőrzés, vagyis az azonosság megerősítése* a cél, ebben az esetben 1:1 megfeleltetésről beszélünk, amikor a rendszer az *egy* személyről készített digitális képet *egy* ellenőrző mintaképpel hasonlítja össze. Ilyen alkalmazás például a határellenőrzésnél a biometrikus útlevélben lévő digitálisan rögzített kép és a jelenlévő útlevélkép, valamint a szintén jelenlévő személy összehasonlítása vagy ilyen a mobiltelefonokba telepített arcfelismerő alkalmazás. Abban az esetben, ha az *azonosítás, vagyis felismertetés* a feladat, 1:*n* vagy *n:n* azonosításról beszélünk, amikor egy (esetleg több) aktuális képhez keressük az elő-

5 Távoli személyazonosítási technikák… i. m.

re létrehozott adatbázisban lévő leginkább megfeleltethető, illetve azonos mintaképet.

Az ellenőrzés, vagyis az azonosság megerősítése (1:1 megfeleltetés) technikailag egyszerűbb, kevesebb hibával terhelt feladat, míg az azonosítás, felismertetés komplexebb, technikailag a variabilitás okán rendkívül összetett tevékenység. Ennek megfelelően a különböző célra különböző képességű, felépítettségű rendszerek létrehozása szükséges.

Egy biometrikus rendszer megbízhatósága, használhatósága szempontjából fontos tényező, hogy mekkora a használt adatbázis *(n)* mérete. Az, hogy mi az optimális méret, sok tényező függvénye. Függ az adatbázisban lévő felvételek paramétereitől (az általános és a speciális képfeldolgozási paraméterektől), az adatbázist alkotó populáció összetételétől, függ az alkalmazott algoritmusoktól amelyeket a rendszer használ. Fontos tudni, hogy az algoritmusokat optimalizált adatbázisokra tesztelik. Ronthatja az arcazonosítás, az adatbázisban keresés, végső soron a döntés hatékonyságát, eredményességét az, hogy a képfeldolgozási algoritmusok az azonosításhoz több sajátosságparamétert használnak, és ezeket általában egy adott képre optimalizálják, majd ezeket használják az adatbázisban lévő különböző képekre. Ebben az esetben nyilvánvaló, hogy nem a minden képre optimalizált sajátosságparaméterek alapján kerül sor a keresésre. Ezt próbálják kiküszöbölni az optimális paraméter keresésére fejlesztett eljárások.

A különböző biometrikus sajátosságot alkalmazó biometrikus rendszereket összehasonlítva az irodalom megállapítja, hogy az arcazonosításnak a legnagyobb a téves elfogadási *(False Accept Rate; FAR)* és a téves visszautasítási *(False Reject Rate; FRR)* rátája[6]. Ezek a mutatók a rendszer megbízhatóságát jellemzik, azt határozzák meg, hogy például egy adott személy esetén milyen valószínűséggel következik be az, hogy a rendszer tévesen fogad el egy pozitív vagy negatív állítást, tévesen azonosít (FAR), illetve hogy milyen valószínűség esetén következik be, hogy tévesen utasít el egy pozitív vagy negatív azonosság állítást (FRR)[7].

A függvényként értelmezett FAR és FRR görbék metszete az azonos hibamérték *(Equal Error Rate; EER)*. Ez az érték a FAR és az FRR eloszlásfüggvények metszéspontja, vagyis az az állapot, amikor FAR = FRR. A két mutató tehát olyan eloszlásfüggvény, amely csak együttesen értelmezhető. A

6 https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/

7 Távoli személyazonosítási technikák… i. m.

biometrikus rendszerek skálázhatók, ami az jelenti, hogy a mutatók változtathatók, de *ha az egyik mutatót növeljük, akkor a másik csökken.*[8]

Az, hogy egy rendszer tévesen azonosít-e (FAR), attól függ, hogy a rendszert működtető algoritmus hány azonosított sajátosság alapján fogadja el a képet. Vagyis meg kell határozni azt a küszöbértéket, amelynél több azonosított sajátosság esetén a képet a rendszer már azonosnak tekinti, ennél a küszöbértéknél kevesebb azonosított sajátosság esetén a rendszer elutasít. Ez tehát a rendszer működésének egyik fontos eleme.

Mint ahogy az előzőekből is kitűnik, az arcazonosításra különböző módszerek, algoritmusok, eszközök használatosak. Az arcazonosításhoz használt algoritmusok, a választott módszerek és eszközök némelyike jobb, míg más megoldások kevésbé pontos eredményt adnak[9].

A használat során azonosított problémák, mint a megvilágítás, a pozíció, az arckifejezés továbbra is a kutatások, fejlesztések fontos területei, úgyszintén az algoritmusok megfelelőségének, alkalmasságának megkerülhetetlen mutatói (a sajátosságok mérhetősége, a mérés pontossága, a találati arány, a hibaszázalék) és a működést meghatározó lényeges paraméterek, mint

– az azonosítás sebessége;
– a műveletek végrehajtásához szükséges memóriakapacitás;
– az automatizáció szintén a fejlesztések kiemelt területei.

De kutatási terület az úgynevezett multimodális rendszerek alkalmazhatóságának kérdése is, ami a különböző biometrikus megoldások kombinálását jelenti, ami az azonosítás biztonsági szintjének a növelése, az azonosítás során felvetődő hibák csökkentése érdekében kap egyre nagyobb hangsúlyt. Ilyen multimodális rendszerek jönnek létre például az arc/hang, az arc/ujjlenyomat, az ujjlenyomat/írisz[10] biometrikus azonosítók kombinálásával.

Ezeknél az alkalmazásoknál szintén fontos szerepük van a megfelelő megválasztott algoritmusoknak és a használni tervezett eszközöknek.

Fontos eleme a biometrikus azonosításnak az adatbázisban tárolt képek minőségének megfelelősége. Az arcfelismerő minták, algoritmusok gyártónként nem kompatibilisek. Ezen túl fontos figyelembe venni azt is, hogy az egyes fejlesztők, gyártók külön mintaadatbázisokra fejlesztenek, erre optimalizálják a rendszereiket, ennek következtében az egyes rendszerek nem feleltethetők meg egymásnak. Nemzetközi ellenőrzések viszonylatában a kompa-

8 http://www.securinfo.hu/termekek/biometria/1160-arc-alapu-azonositas-a biometriaban.html
9 Proyecto Fin de Carrera: Face Recognition Algorithms, 16 June 2010.
10 https://findbiometrics.com/solutions/multimodal-biometrics/

tibilitás, a hatékonyság, az ellenőrzések eredményessége érdekében cél, hogy minél szabályozottabb, egységesebb képformátumokban tárolják az összehasonlítandó biometrikus adatot. Az arcfelismeréshez a kép tárolása pixelgrafikus formákban (például: *BMP*, 24 bit színmélységű, bittérképes, nem tömöríthető képformátum; *JPEG,* 24 bit színmélységű, veszteségesen vagy veszteségmentesen tömöríthető képformátum; *PNG,* veszteségmentesen tömöríthető RGB képet adó képformátum) történhet, amelyek képpontokból, úgynevezett pixelekből építik fel a képet[11]. A Nemzetközi Polgári Repülési Szervezet *(International Civil Aviation Organization; ICAO)* által preferált, standardizált képi adat a 300 dpi-s színes kép, amely kilencven pixelből áll a szemek között, és a mérete kb. 640 kB, pixelenként 24 bittel. Ez a kép jelentősen tömöríthető JPEG/JPEG2000 technikát alkalmazva, a tömörítési eljárás történhet veszteséggel, illetve veszteségmentesen.

Megjegyzendő, hogy az e-útlevelekben lévő, a chipen tárolt arcképek tömörítésének mértéke 15 és 20 kB közé esik. A megengedett minimum 12 kB[12].

A standardizált képformátum kiküszöbölheti, vagy legalábbis mérsékli a különböző algoritmusokkal működő rendszerek esetében az azonosítási anomáliákat.

Napjainkban az arcazonosítás, ezen belül az automatikus arcazonosítás, adatbázisban való keresés számos biztonsági területen új lendületet adott ennek a biometrikus azonosítási programnak. Lásd az egyesült államokbeli Biometrikus Exit programot[13], amelynek többféle biometrikus azonosítási megoldása volt napirenden évek óta, de a technológia hibái, és esetenként „kísérleti megoldásai" ellenére – a repülőtéri kapuknál végrehajtható tömeges ellenőrzés lehetősége, az arc ellenőrzésének egyszerű kivitelezhetősége miatt – végül az arcazonosítási technológia bevezetésére került sor.

Új eljárások, mint a 3D felismerés[14], amely esetében a 3D szenzorokkal gyűjtött adatok teljesebb körű információt adnak az arc sajátosságairól, mert csökken a megvilágításra, az árnyékolásra és a nem megfelelő pozícióra visszavezethető hiba, vagy az arckifejezés variabilitásának csökkentését célzó módszerek, a bőr textúrájának analízise, a hőképek analízise mesterséges intelligencia segítségével (arcfelismerés sötétben)[15], illetve a különböző módszerek kombinálása napjainkban új irányokat nyithat meg a biztonsági területeken.

11 Távoli személyazonosítási technikák… i. m.

12 ICAO Doc 9303… i. m.

13 Ravi Das: The controversial comeback of facial recognition. Keesing Journal of Documents and Identity, vol. 54, 2017

14 http://www2.mit.bme.hu/services/vimm3241/tanul/beadott/regi/SzigetvariMadai/

15 https://www.sciencedaily.com/releases/2018/04/180416142443.htm

Fontos tehát az azonosítás/felismerés módszereinek, az alkalmazás körülményeinek, a lehetséges hibáknak a pontos, ha nem is teljes körű feltérképezése, a kapcsolódó kockázatoknak az elemzése ahhoz, hogy megfelelő döntés szülessen egy módszer kiválasztásánál vagy egy rendszer létrehozásánál.

Mivel ehhez többnyire csak korlátozott információ áll rendelkezésre, mert a gyártók az egyedi fejlesztésű rendszereikről csak kevés információt osztanak meg, és mert az egyes rendszereket optimális körülményekre tesztelik, általában kisszámú adatbázissal, ezért lényeges a tervezett körülményekre és paraméterekre saját tesztek elvégzése, az eredmények értékelése és a kockázatok megállapítása.